AMENDMENTS TO THE CLAIMS

1. (Currently amended) An anonymous electronic voting system comprising:

voter terminals for receiving a list of combinations of candidate [[name]] names and encrypted candidate [[name]] names, to transmit [[said]] an encrypted candidate name of a selected candidate via a network;

at least one encryption server for receiving and re-encrypting said encrypted candidate name of the selected candidate to create encrypted voting data, and returning said encrypted voting data to said voter terminal having transmitted said encrypted candidate name of the selected candidate;

a voting server for receiving said encrypted voting data from said voter terminal to create a list of effective encrypted voting data from among said received encrypted voting data, and transmitting said created list of said effective encrypted voting data via said network; and

a decryption server for decrypting said list of said effective encrypted voting data received from said voting server, to create and transmit via said network a list of plaintext candidate names rearranged from said list of said effective encrypted voting data,

wherein said voting server receives said list of said plaintext candidate names from said decryption server, to tally vote results based on said list of said received candidate names.

2. (Previously presented)) The anonymous electronic voting system according to claim 1, further comprising another voter terminal including an encryption means for encrypting a candidate name of a selected candidate to create an encrypted candidate name.

3.-5. (Canceled)

6. (Previously presented) The anonymous electronic voting system according to claim 1, further comprising an authentication server, wherein:

said voter terminal includes an intra-organization-signature creation means for creating an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key,

3

said authentication server receives said encrypted voting data, said intra-organization identification data, and said intra-organization digital signature from said voter terminal, to certify said intra-organization digital signature based on a public key; and

said voting server acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

7. (Previously presented) An anonymous electronic voting system comprising:

voter terminals connected to a network;

a first encryption server including a first data conversion means for creating a first encryption parameter for each of said voter terminals from public information, and transmitting said first parameter to said voter terminals;

a second encryption server including a second data conversion means for creating a second encryption parameter, and transmitting said second parameter to said voter terminals;

a voting server for receiving encrypted voting data from said voter terminals to create a list of effective encrypted voting data from among said received encrypted voting data, and transmitting said created list of said effective encrypted voting data via said network; and

a decryption server for decrypting said list of said effective encrypted voting data received from said voting server, to create and transmit via said network a list of plaintext candidate names rearranged from said list of said effective encrypted voting data, wherein:

names from said decryption server, to tally voted results based on said list of said received candidate names; and said

voter terminals each include an encryption means for encrypting voting contents based on said first and second encryption parameters to create encrypted voting data, and transmits said encrypted voting data to said voting server.

8.-9. (Canceled)

10. (Previously presented) The anonymous electronic voting system according to claim 7, wherein said first encryption server and said voting server operate on a common server.

4

11. (Previously presented) The anonymous electronic voting system according to claim 7, wherein:

said voter terminals create, in addition to said encrypted voting data, encryption-certificate data, and transmits the same to said voting server;

said voting server, upon completing verification of legitimacy by verifying at least said encryption-certificate data, acknowledges corresponding said encrypted voting data as said effective encrypted voting data.

12. (Currently amended) An anonymous electronic voting method using a voting server, a voter terminal for voting therethrough by a voter, an encryption server, and a decryption server, said comprising the steps of:

transmitting from said voting server a list of combinations of candidate [[name]] names and encrypted candidate [[name]] names obtained by encrypting said candidate [[name]] names to said voter terminal via a network;

transmitting from said voter terminal an encrypted candidate name, which is paired with a candidate name selected by a voter, to said encryption server;

re-encrypting said encrypted candidate name in said encryption server to create encrypted voting data, and transmitting said encrypted voting data to said voter terminal having transmitted said encrypted candidate name;

transmitting from said voter terminal said encrypted voting data, which is received from said encryption server, to said voting server;

receiving said encrypted voting data in said voting server to create and transmit a list of effective encrypted voting data;

decrypting said list of said encrypted voting data in said decryption server to create a list of plaintext candidate names rearranged; and

receiving said list of said plaintext candidate names in said voting server to tally vote results based on said list of said received candidate names.

13. (Previously presented) The anonymous electronic voting method according to claim 12, further comprising the steps of:

receiving from said voter terminal said encrypted voting data and identification data in an authentication server to certify said encrypted voting data based on identification data stored in a storage device and transmitting said encrypted voting data; and

acknowledging in said voting server at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

14. (Previously presented) The anonymous electronic voting method according to claim 12, further comprising the steps of:

creating in said voter terminal an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key;

receiving in said authentication server said encryption voting data, intra-organization identification server and intra-organization digital signature from said voter terminal;

acknowledging in said voting server at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

15. (Previously presented) The anonymous electronic voting method according to claim 12, wherein said step of re-encrypting said encrypted candidate name is the step of consecutively multiple-encrypting said encrypted candidate name in a group of encryption servers.

16. (Previously presented) The anonymous electronic voting method according to claim 12, wherein:

each of said combinations in said list includes, in addition to said candidate name and said encrypted candidate name, certificate data for certifying that said candidate name is legitimately encrypted; and

said encryption server creates, in addition to said encrypted voting data, certificate data for certifying legitimacy of said encrypted voting data, to return the same to said voter terminal.

6

17. (Previously presented) An anonymous electronic voting method comprising the steps of:

creating in a first encryption server a first encryption parameter for each of voter terminals from public information, and transmitting said first parameter to said voter terminals;

creating in a second encryption server a second encryption parameter for each of said voter terminals from said public information, and transmitting said second parameter to said voter terminals;

encrypting voting contents of a voter in said voter terminal based on said first and second encryption parameters to create encrypted voting data, and transmitting said encrypted voting data to said voting server;

creating a list of effective encrypted voting data from among said received encrypted voting data in said voting server and transmitting said created list of said effective encrypted voting data via said network;

decrypting in a decryption server said list of said effective encrypted voting data received from said voting server, to create and transmit via said network a list of plaintext candidate names rearranged from said list of said effective encrypted voting data; and

receiving in said voting server said plaintext candidate names, to tally voted results based on said list of said received candidate names.

18. (Previously presented) The anonymous electronic voting method according to claim 17, wherein said encryption voting data creating step creates encryption-certificate data certifying legitimacy of said encrypted voting data, further comprising the step:

after verifying legitimacy in said voting server by verifying at least said encryption-certificate data, acknowledging corresponding said encrypted voting data as said effective encrypted voting data.

19. (Previously presented) The anonymous electronic voting method according to claim 17, further comprising the steps of: receiving in a certification server said encrypted voting data and identification data from said voter terminal, and certifying said encrypted voting data based on

7

identification data stored in a storage device; and acknowledging in said voting server at least said encrypted voting data affixed with said certificate data as said effective voting data.

20. (Previously presented) The anonymous electronic voting method according to claim 17, further comprising the steps of:

creating in said voter terminal an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key;

receiving in said authentication server said encrypted voting data, said intra-organization identification data, and said intra-organization digital signature from said voter terminal, to certify said intra-organization digital signature based on a public key; and

acknowledging in said voting server at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

21. (Previously presented) The anonymous electronic voting method according to claim 7, wherein said at least one second encryption server include a group of second encryption servers, and said voter terminals each include an encryption means for multiple-encrypting said voting contents based on said first parameter and said second parameters transmitted from said group of second encryption servers to create said encrypted voting data and transmit said encrypted voting data to said voting server.

22. (Previously presented) The anonymous voting method according to claim 17, wherein said creating of said second parameter includes creating a plurality of said second parameter in a group of second encryption servers, and said encrypting of said voting contents includes multiple-encrypting said voting contents based on said first parameter and a plurality of said second parameters.

23. (Previously presented) The anonymous electronic voting system according to 1 further comprising an authentication server including a storage device for storing a list of identification data of voters or voter terminals included in a voter list, said authentication server receiving said encrypted voting data and identification data from said voter terminal to certify said

8

encrypted voting data based on said identification data stored in said storage device, wherein said voting server acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

24. (Previously presented) The anonymous electronic voting system according to any claim 1, wherein said at least one encryption server include a group of encryption servers for consecutively multiple-encrypting said encrypted candidate name, and said voting server receives said encrypted voting data multiple-encrypted by said group of said encryption servers.

25. (Previously presented) The anonymous electronic voting system according to claim 1, wherein:

each of said combinations in said list includes, in addition to said candidate name and said encrypted candidate name, certificate data for certifying that said candidate name is legitimately encrypted; and

said encryption server creates, in addition to said encrypted voting data, certificate data for certifying legitimacy of said encrypted voting data, to return the same to said voter terminal.

26. (Previously presented) The anonymous electronic voting system according to claim 7, further comprising an authentication server including a storage device for storing a list of identification data of voters or voter terminals included in a voter list, said authentication server receiving said encrypted voting data and identification data from said voter terminals to certify said encrypted voting data based on said identification data stored in said storage device, wherein said voting server acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

27. (Previously presented) The anonymous electronic voting system according to claim 7, further comprising an authentication server, wherein:

said voter terminals each include an intra-organization-signature creation means for creating an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key,

9

said authentication server receives said encrypted voting data, said intra-organization identification data, and said intra-organization digital signature from said voter terminal, to certify said intra-organization digital signature based on a public key; and

said voting server acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.